REMARKS

Claims 15 to 29 are now pending. Claims 18, 20, 23, and 25 to 29 have been amended to correct minor informalities. Fig. 3 has been amended to correct a minor informality. New Figs. 4 and 5 have been added. The Specification has been amended accordingly to account for the Figs. 3, 4 and 5. No new matter has been added.

Applicants respectfully request reconsideration of the present application in view of this response.

Regarding paragraph one (1) of the Office Action, the drawings were objected to for including reference numbers 130, 132, 134, 135, 138 and 140 in Fig. 3 which were not mentioned in the Specification. In accordance with the Examiner's suggestion, the Specification was amended to cite the reference numbers of Fig. 3. In addition, latch 134 of Fig. 3 was amended to read latch 135 since another element used the reference number 134. No new matter has been added. Applicants respectfully submit that Fig. 3 and the Specification as amended are allowable; and, withdrawal of the objection to the drawings is respectfully requested.

Regarding paragraph two (2) of the Office Action, the drawings were objected to for not showing every feature of the invention specified in the claims. Specifically, "input data," "chip card" and "security module" of claim 15 were stated as not included in the drawings. In fact, Applicants respectfully submit that those features of method claim 15 are included in the drawings at Fig. 1 – "input data" is shown at reference number 106, "chip card" is shown at reference number 102, and "security module" is shown at reference number 104. In addition, the Specification supports Fig. 1 at page 3, lines 5-16. Applicants appreciate the Examiner's diligence in this matter and apologize if such features were not readily seen in Fig. 1 and the Specification. If the Examiner wishes additional drawings to show the same features, Applicants would appreciate recommendations from the Examiner regarding providing a non-identical drawing.

Applicants have submitted above new Fig. 4 which shows the feature "additional feedback" being tapped off from claims 25 and/or 26. No new matter has been added. New Fig. 4 also shows the feature "second" of the at least one second downstream counter of claims 27 as reference number 136b. Applicants have also submitted above new Fig. 5 which shows the feature of XOR from claim 28. No new matter has been added. The Specification has been amended accordingly.

Accordingly, Applicants respectfully submit that the drawings (Fig. 1), the proposed drawing corrections (Fig. 3) and the new drawings (Figs. 4 and 5) do not add new matter, and

overcome any objections to the drawings. Applicants respectfully submit that all Figs. 1 to 5 are allowable; and, withdrawal of the objection to the drawings is respectfully requested.

Regarding paragraphs three (3) and four (4) of the Office Action, claims 20 and 24 to 29 were rejected under 35 U.S.C. § 112, first paragraph. Specifically, claim 20 was rejected due to it not being clear where the disclosure for selecting the first number of clock pulses was, as claimed. Applicants respectfully submit that the disclosure for this feature is seen in the Specification at page 5, lines 1-20, page 4, lines 9-23 and page 3, lines 18-31. In addition, the Specification has been amended to include this statement for further clarification. Support for the amendment can be found in claim 20. Specifically, claims 24 to 29 were rejected for using terms such as "may" and "for example." Although believed not necessary, in response to the Examiner's rejection, Applicants have amended the Specification to not recite "may" in certain paragraphs in the Detailed Description since such language appears to cause confusion. Applicants respectfully submit these amendments, as well as the other amendments submitted above, further clarify the multiple embodiments of the present invention. Applicants are their own lexicographer and use "exemplary embodiment" and "for example" to suggest various alternative embodiments – all preferred – of the present invention. Applicants respectfully submit that they are not required to specifically point out a "preferred" embodiment. However, at the same time, Applicants have indicated throughout the Specification many desired embodiments of the present invention. Applicants respectfully submit that the many amendments to the Specification now provide further clarification to the reader.

Specifically, claim 25 was rejected because the Specification does not include a description of the latch. Figs. 3, 4 and 5, and the Specification as amended above, show and describe an embodiment of the latch.

Accordingly, in light of the above explanations and amendments, Applicants respectfully submit that the amended Specification and claims 20 and 24 to 29 are in condition for allowance; and, withdrawal of the rejection under 35 U.S.C. § 112, first paragraph, of claims 20 and 24 to 29 is respectfully requested.

Regarding paragraphs five (5) and six (6) of the Office Action, claims 18 and 24 to 29 were rejected under 35 U.S.C. § 112, second paragraph. Specifically, claim 18 was rejected for lacking antecedent bases for "different contents" and "in calculating an authentication token." Claim 18 has been amended above to correct the antecedent bases. Specifically, claim 20 was rejected for lacking antecedent basis for "in calculating an authentication token." Claim 20 has been amended above to correct the antecedent basis. Claim 24 was

rejected for reciting "counter" instead of "first counter." Claim 24 has been amended in accordance with the Examiner's recommendation. Claims 25 to 28 were rejected for reciting "the additional feedback" without antecedent support. Claims 25 to 28 have been amended to correct the antecedent basis. No comment was made with respect to claim 29.

Accordingly, in light of the amendments to the claims, Applicants respectfully submit that claims 18 and 24 to 29 are in condition for allowance; and, withdrawal of the rejection under 35 U.S.C. § 112, second paragraph, of claims 18 and 24 to 29 is respectfully requested.

Regarding paragraphs seven (7) and eight (8) of the Office Action, claims 15 to 23 have been rejected under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 6,434,238 to Chaum et al. (the "Chaum reference").

The Chaum reference purportedly concerns a multipurpose transaction card system comprising an issuer, one or more cards, one or more terminals, and one or more acquires, communicating using a variety of cryptographic confidentiality and authentication methods. Abstract, lines 1-5. The Chaum reference refers to cards authenticating messages using public key based cryptography without themselves performing the extensive computations usually associated with such cryptography. Abstract, lines 5-8. The Chaum reference further refers to maintaining integrity of complex transaction sequences and plural card storage updates even during intentionally generated interruptions and/or modifications of data transmitted between the card and terminal. Abstract, lines 8-11. The Chaum reference states that the cards do not reveal any information to the terminal which is not directly necessary for the transaction or any information to which the terminal should not have access, though externally measurable aspects of its behavior. Abstract, lines 11-15. The Chaum reference refers to "open to buy" being maintained on the card.

Claim 15 recites a method for loading input data into a program when performing a cash transaction authentication between and electronic cash chip card and a security module, the chip card including a stored credit balance, including the features of:

> debiting a requested cash amount from the chip card using a security function;
> adding and storing the requested cash amount in a cash amount summing counter of the security module,
> subdividing the input data into a plurality of data blocks;
> loading the plurality of data blocks into a linear-feedback shift register for performing the program, the linear-feedback shift register having at least one non-linear function cryptographically enhanced using at least one downstream counter;
> introducing at least one additional feedback into the linear-feedback shift register following the at least one downstream counter; and
> switching off the at least one additional feedback after a predefined first number of pulses of an associated clock.

In contrast, the Chaum reference does not include at least the features of subdividing the input data into a plurality of data blocks; loading the plurality of data blocks into a linear-feedback shift register for performing the program, the linear-feedback shift register having at least one non-linear function cryptographically enhanced using at least one downstream counter; introducing at least one additional feedback into the linear-feedback shift register following the at least one downstream counter; and switching off the at least one additional feedback after a predefined first number of pulses of an associated clock, as in claim 15. Instead, the Chaum reference refers to a smart card being used as an endorser, the i/o interface communicating with the outside world though an interface link (col. 13, lines 56 et seq.), and the smart card in a situation where there is an issuer, card, terminal and an acquirer. In such situation, as referred to by the Chaum reference, the card is produced and typically initialized by the issuer using a data channel. Col. 20, lines 1-15. And, according to the Chaum reference, before a transaction is made, a data channel is established between the card and the terminal, via which various transaction can be perfomed, some offline. Col. 20, lines 20-33. The acquirer collects the information, according to the Chaum reference, from one or more terminals and optionally handles some or all of the clearing and settlement of the transactions the terminal participated in, collecting the cryptographic proofs of payments from the terminals, updating system parameters in the terminals, etc. Col. 20, lines 34-47.

Accordingly, it is respectfully submitted that claim 15 is allowable over the Chaum reference. Since claims 16 to 23 depend from claim 15, it is respectfully submitted those claims are allowable over the Chaum reference for at least the same reasons as for claim 15.

Applicants respectfully request withdrawal of the rejection of claims 15 to 23 under 35 U.S.C. § 103(a) in view of the Chaum reference.

Moreover, to reject a claim as obvious under 35 U.S.C. § 103, the prior art must disclose or suggest each claim element and it must also provide a motivation or suggestion for combining the elements in the manner contemplated by the claim. (See Northern Telecom, Inc. v. Datapoint Corp., 908 F.2d 931, 934 (Fed. Cir. 1990), cert. denied, 111 S. Ct. 296 (1990); In re Bond, 910 F.2d 831, 834 (Fed. Cir. 1990)).

The Federal Circuit in the case of In re Kotzab has made plain that even if a claim concerns a "technologically simple concept" -- which is not even the case here, there still must be some finding as to the "specific understanding or principle within the knowledge of a skilled artisan" that would motivate a person having no knowledge of the claimed subject matter to "make the combination in the manner claimed", stating that:

> In this case, the Examiner and the Board fell into the hindsight trap. The idea of a single sensor controlling multiple valves, as opposed to multiple sensors controlling multiple valves, is a technologically simple concept. **With this simple concept in mind, the Patent and Trademark Office found prior art statements that in the abstract appeared to suggest the claimed limitation. But, there was no finding as to the specific understanding or principle within the knowledge of a skilled artisan that would have motivated one with no knowledge of Kotzab's invention to make the combination in the manner claimed.** In light of our holding of the absence of a motivation to combine the teachings in Evans, we conclude that the Board did not make out a proper *prima facie* case of obviousness in rejecting [the] claims . . . under 35 U.S.C. Section 103(a) over Evans.

(See In re Kotzab, 55 U.S.P.Q.2d 1313, 1318 (Federal Circuit 2000) (citations omitted, italics in original, emphasis added)). Here, there have been no such findings. *In addition*, with respect to the above-identified application, Applicants request some sort of evidence and/or affidavit from the Patent Office regarding the Patent Office's assertions of what it suggests is obvious to one of ordinary skill in the art.

In view of the above amendments and remarks, Applicants respectfully request allowance of claims 15 to 23.

Regarding paragraphs nine (9) and ten (10) of the Office Action, claims 24 and 29 were rejected under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,377,270 to Koopman, Jr. et al. (the "Koopman reference").

The Koopman reference purportedly concerns a cryptographic authentication of transmitted messages using pseudorandom numbers. Title. The Koopman reference refers to an automobile door lock receiver module and a plurality of keychain fob transmitter units containing identification numbers, secret initial values and secret feedback masks so as to authenticate encrypted messages from any of the assigned fobs, indicative of commands registered by closing switches on the fob. Abstract, lines 1-6. The Koopman reference further refers to each fob being synchronized with the receiving module by means of a truly random number concatenated with a secret initial value and encrypted, through a linear feedback shift register or other operations. Abstract, lines 6-10. The Koopman reference states that a second secret initial value is encrypted and command bits are exclusive Ored into the low order bit positions, the two encrypted numbers are concatenated and encrypted to form a key word which is transmitted with the fob ID. Abstract, lines 10-14. The Koopman reference further refers to decrypting to recover the truly random number and the secret initial

value concatenated therewith, the truly random number being compared with the previously received random numbers in order to avoid copying of recently transmitted synchronization commands. Abstract, lines 14-20. The Koopman reference further refers to successive lock-related commands utilizing the number encrypted from the truly random number and the second secret initial value as starting values, employing a pseudorandom number of encryption iterations, a half-second delay between responses mitigates gaining access through numerical trials. Abstract, lines 20-25. The Koopman reference then refers to an authentication panic alarm command operating the headlights and horn of the vehicle, without altering the synchronization. Abstract, lines 25-28.

Claim 24 recites a device for loading input data into a program when performing an authentication using a cryptographic MAC function, including:

> a first counter;
> a linear-feedback shift register having a nonlinear feed-forward function for reading off from the linear-feedback shift register, and for influencing an output of the linear feedback shift register using the first counter, the linear-feedback shift register forming at least part of a circuit;
> at least one second counter for performing the program, the at least one second counter connected downstream of the linear-feedback shift register; and
> at least one additional non-linear feedback shift register for cryptographically enhancing the circuit and being connected to the circuit, the at least one additional nonlinear feedback shift register being disconnectable.

In contrast, the Koopman reference does not identically disclose (as it must for anticipation) at least the features of: a linear-feedback shift register having a nonlinear feed-forward function for reading off from the linear-feedback shift register, and for influencing an output of the linear feedback shift register using the first counter, the linear-feedback shift register forming at least part of a circuit; at least one second counter for performing the program, the at least one second counter connected downstream of the linear-feedback shift register; and at least one additional non-linear feedback shift register for cryptographically enhancing the circuit and being connected to the circuit, the at least one additional nonlinear feedback shift register being disconnectable. The Koopman reference at cols. 5-7, cited as support in the Office Action, refers to a receiver module being connected to the locks of an automobile, but before a fob can be utilized to operate the locks, synchronization must occur. The synchronization begins with two secret initial (seed) values for the fob 16 located in a 20 bit linear feedback shift register 53 and a 19 bit linear feedback shift register 54, and suitable feedback masks for each of the registers available at the input of corresponding feedback exclusive Ors. See Fig. 1. The initial synchronization includes 20 iterations of the shift

register and at least 19 iterations of the second shift register; and in each cycle, the high order bit is transferred by a line to the low order bit and is exclusively Ored with those bits of the shift registers identified by bits in the feedback masks, to form the next higher order bits within the shift registers; the feedback mask has to represent a suitable polynomial so as to provide a maximal length code having degree N. Id. In general, the pseudorandom number generator need not be reversible; a reversible generator being one where given the current pseudorandom number and complete knowledge of the generation process, the previous pseudorandom number may be determined. Id.

Accordingly, it is respectfully submitted that claim 24 is allowable over the Koopman reference. Since claim 29 depends from claim 24, it is respectfully submitted claim 29 is allowable over the Koopman reference for at least the same reasons as for claim 24.

Applicants respectfully request withdrawal of the rejection of claims 24 and 29 under 35 U.S.C. § 102(b) in view of the Koopman reference.

Moreover, to reject a claim under 35 U.S.C. § 102(b), the Office must demonstrate that each and every claim limitation is identically disclosed in a single prior art reference. (See *Scripps Clinic & Research Foundation v. Genentech, Inc.*, 18 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 1991)). Still further, not only must each of the claim limitations be identically disclosed, an anticipatory reference must also enable a person having ordinary skill in the art to practice the claimed invention, namely the inventions of the rejected claims. (See *Akzo, N.V. v. U.S.I.T.C.*, 1 U.S.P.Q.2d 1241, 1245 (Fed. Cir. 1986)). In particular, it is respectfully submitted that, at least for the reasons discussed above, the Koopman reference relied upon would not enable a person having ordinary skill in the art to practice the subject matter of the rejected claims 24 and 29, as discussed above.

In summary, it is respectfully submitted that all of claims 15 to 29 of the present application are allowable at least for the foregoing reasons.

CONCLUSION

In view of all of the above, it is believed that the objections to the drawings and Specification, and the rejections of claims 15 to 29, under 35 U.S.C. §§ 112, 102(b) and 103(a), have been obviated, and that these currently pending claims are allowable. It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

The Examiner is respectfully encouraged to contact the undersigned via telephone if such communication might advance allowance of the present application.

Respectfully submitted,

By: Linda M. Saltiel
Reg. No. 47084

Dated: September 30, 2003

By: Richard L. Mayer
Richard L. Mayer (Reg. No. 22,490)

KENYON & KENYON
One Broadway
New York, New York 10004
(212) 425-7200

CUSTOMER NO. 26646

[ANNOTATED SHEET SHOWING CHANGES]

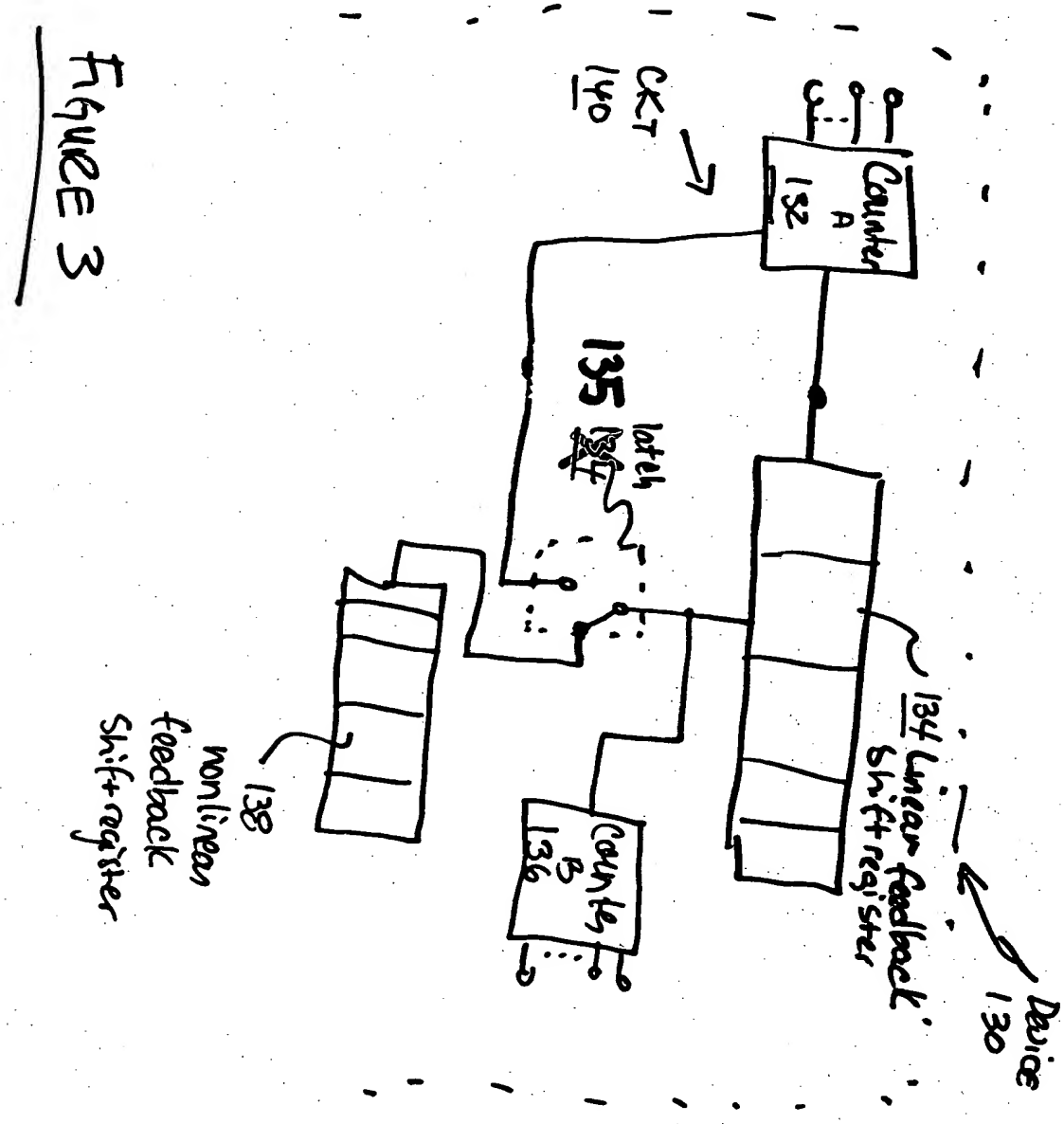

Figure 3